

INFN-AAI SAML & OIDC



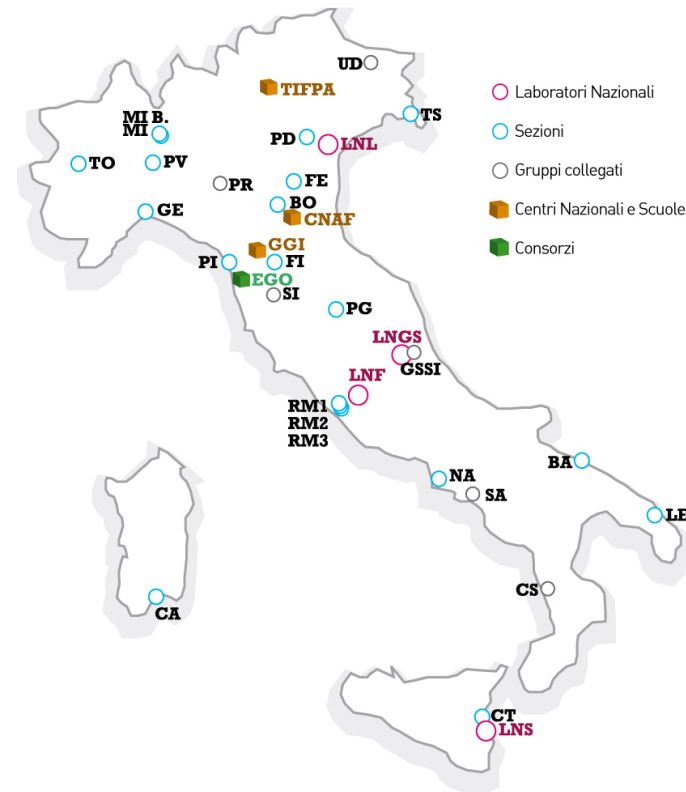
Workshop GARR 2019 – NET Makers
Roma 9 ottobre 2019

Enrico M. V. Fasanelli

Istituto Nazionale di Fisica Nucleare



- 26 Sezioni
- 4 Laboratori Nazionali
- 6 Gruppi Collegati
- 3 Centri Nazionali
- Amministrazione Centrale
- Ufficio di Presidenza
- Consorzio EGO



INFN: AuthN & AuthZ pre INFN-AAI (2008)

- 26 Sezioni
 - 4 Laboratori Nazionali
 - 6 Gruppi Collegati
 - 3 Centri Nazionali
 - Amministrazione Centrale
 - Ufficio di Presidenza
 - Consorzio IN2P3
- 41 Strutture**
~30 AuthN & AuthZ
>10 DB utenti in AC



INFN – AuthN & AuthZ con AAI

- Singolo DB Identità Digitali e ruoli
 - DB autoritativo anche per processi amministrativi

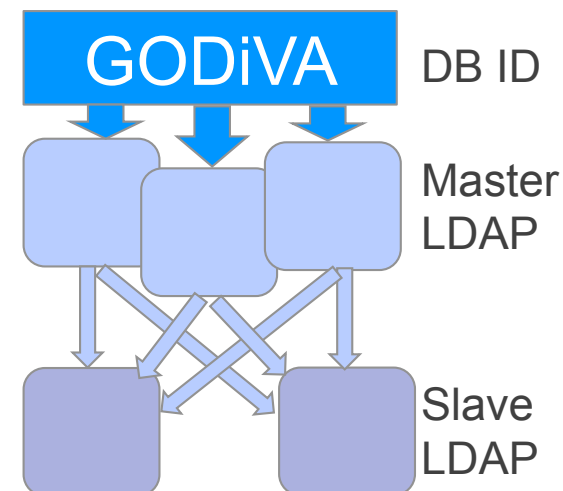


GODiVA

DB ID

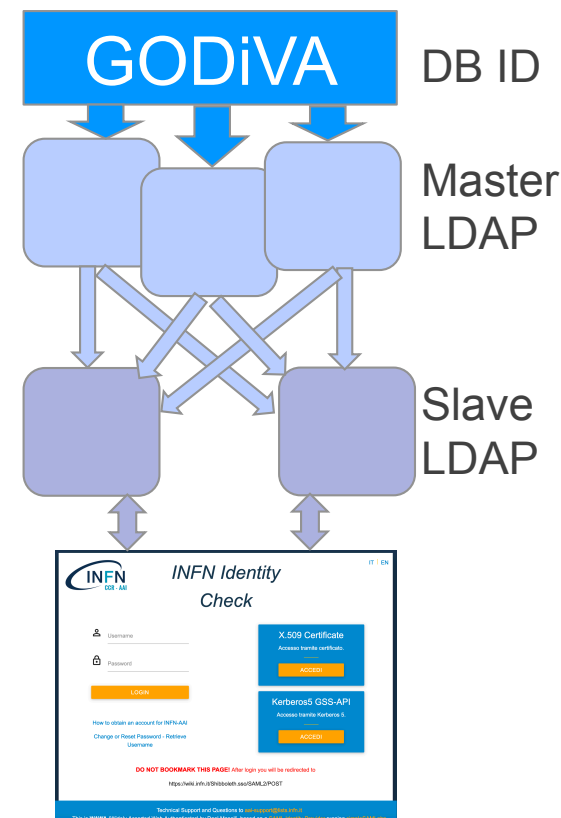
INFN – AuthN & AuthZ con AAI

- Singolo DB Identità Digitali e ruoli
 - DB autoritativo anche per processi amministrativi
- AuthN & AuthZ via LDAP (+Kerberos5)
 - 389-DS multi-master + n slaves
 - 2 master @LNF + 1 master @CNAF
 - 1 slave @LNF + 1 slave @CNAF



INFN – AuthN & AuthZ con AAI

- Singolo DB Identità Digitali e ruoli
 - DB autoritativo anche per processi amministrativi
- AuthN & AuthZ via LDAP (+Kerberos5)
 - 389-DS multi-master + n slaves
 - 2 master @LNF + 1 master @CNAF
 - 1 slave @LNF + 1 slave @CNAF
- IdP SAML basato su SimpleSAMLphp
 - 2 IdP @LNF + 1 hot-standby @CNAF



INFN – AuthN

- Singolo DB Identificativo
- DB autoritativo amministrativi
- AuthN & AuthZ via
- 389-DS multi-master
 - 2 master @LNF
 - 1 slave @LNF
- IdP SAML basato su Shibboleth
 - 2 IdP @LNF +



INFN Identity Check

 Username

 Password

LOGIN

[How to obtain an account for INFN-AAI](#)

[Change or Reset Password - Retrieve Username](#)

X.509 Certificate
Accesso tramite certificato.
ACCEDI

Kerberos5 GSS-API
Accesso tramite Kerberos 5.
ACCEDI

DO NOT BOOKMARK THIS PAGE! After login you will be redirected to <https://wiki.infn.it/Shibboleth.sso/SAML2/POST>

Technical Support and Questions to aai-support@lists.infn.it
This is **WAWA** (Widely Assorted Web Authenticator) by Dael Maselli, based on a [SAML Identity Provider](#) running [simpleSAMLphp](#)



DB ID

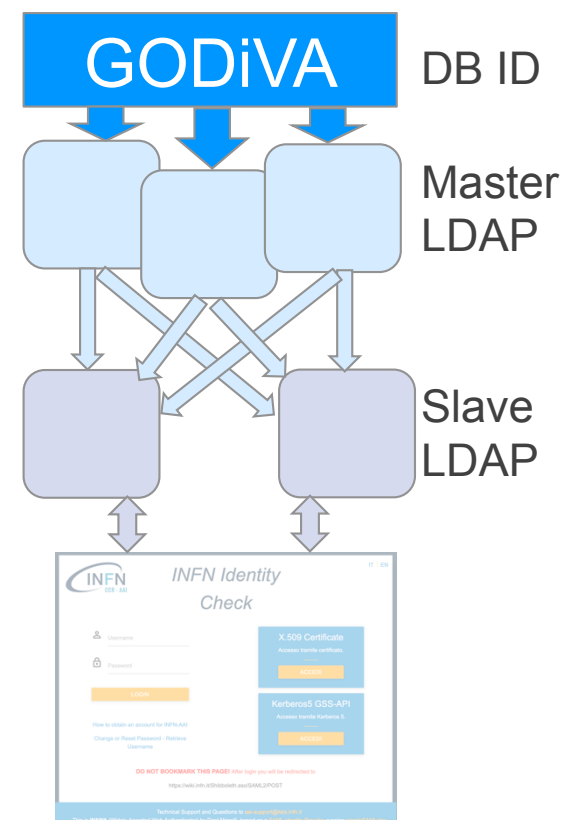
Master LDAP

Slave LDAP

INFN-AAI

INFN – AuthN & AuthZ con AAI

- Singolo DB Identità Digitali e ruoli
 - DB autoritativo anche per processi amministrativi
- AuthN & AuthZ via LDAP (+Kerberos5)
 - 389-DS multi-master + n slaves
 - 2 master @LNF + 1 master @CNAF
 - 1 slave @LNF + 1 slave @CNAF
- IdP SAML basato su SimpleSAMLphp
 - 2 IdP @LNF + 1 hot-standby @CNAF



NonSoloSAML

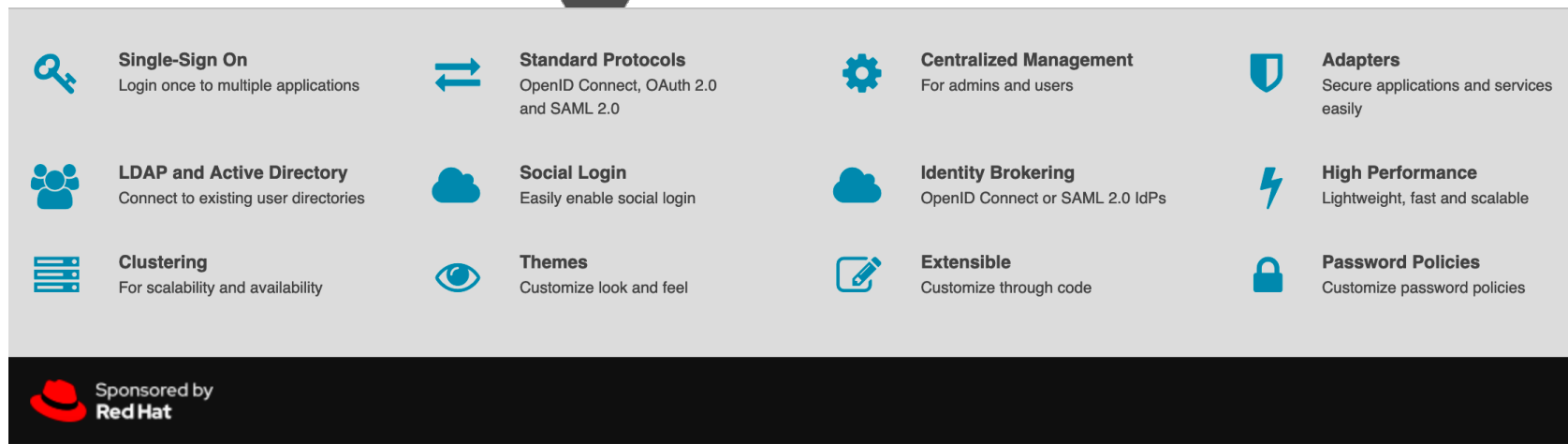
- Sempre più pressante la necessità di supporto per OIDC
- Vincoli: GODiVA e SimpleSAMLphp
 - Provato senza successo il modulo OIDC di RedIRIS

NonSoloSAML

- Sempre più pressante la necessità di supporto per OIDC
- Vincoli: GODiVA e SimpleSAMLphp
 - Provato senza successo il modulo OIDC di RedIRIS
- Ci siamo imbattuti in  **KEYCLOAK**

NonSoloSAML

- Sempre più pressante la necessità di supporto per OIDC
- Vincolo: SimpleSAMLphp
 - Provato senza successo il modulo OIDC di RedIRIS
- Ci siamo imbattuti in 

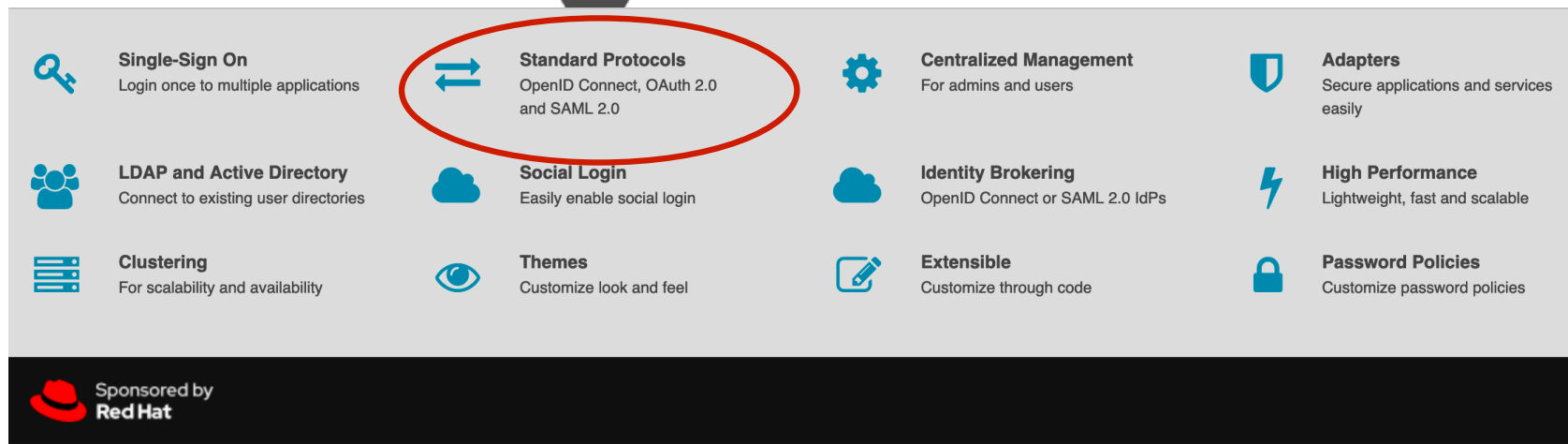


 Single-Sign On Login once to multiple applications	 Standard Protocols OpenID Connect, OAuth 2.0 and SAML 2.0	 Centralized Management For admins and users	 Adapters Secure applications and services easily
 LDAP and Active Directory Connect to existing user directories	 Social Login Easily enable social login	 Identity Brokering OpenID Connect or SAML 2.0 IdPs	 High Performance Lightweight, fast and scalable
 Clustering For scalability and availability	 Themes Customize look and feel	 Extensible Customize through code	 Password Policies Customize password policies

 Sponsored by
Red Hat

NonSoloSAML

- Sempre più pressante la necessità di supporto per OIDC
- Vincolo: SimpleSAMLphp
 - Provato senza successo il modulo OIDC di RedIRIS
- Ci siamo imbattuti in 



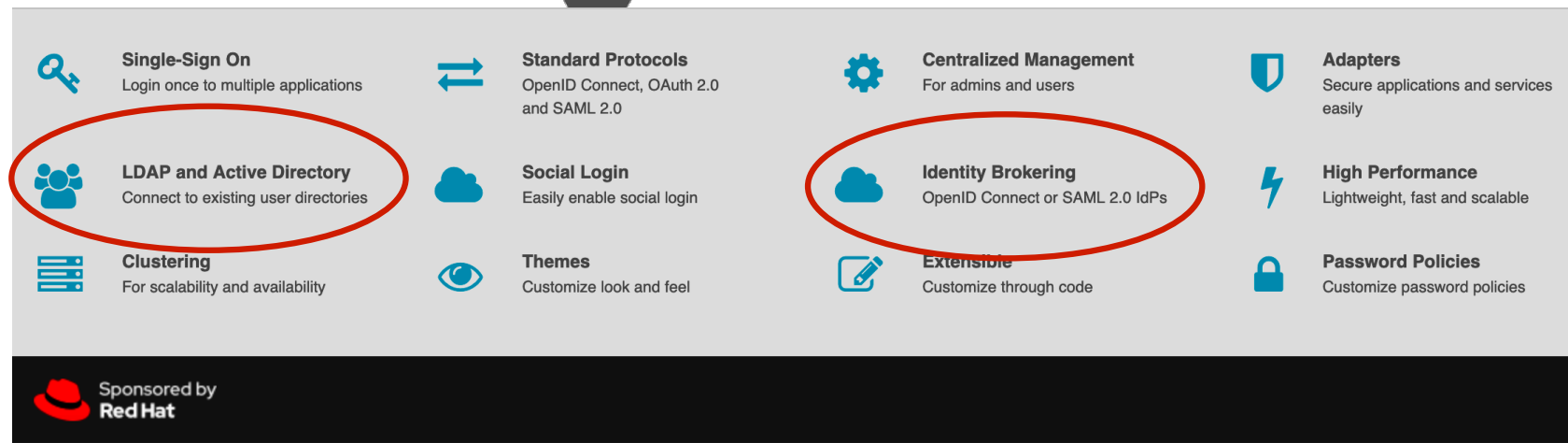
A grid of 12 features for Keycloak, arranged in 3 rows and 4 columns. Each feature has an icon, a title, and a description. The 'Standard Protocols' feature is circled in red.

 Single-Sign On Login once to multiple applications	 Standard Protocols OpenID Connect, OAuth 2.0 and SAML 2.0	 Centralized Management For admins and users	 Adapters Secure applications and services easily
 LDAP and Active Directory Connect to existing user directories	 Social Login Easily enable social login	 Identity Brokering OpenID Connect or SAML 2.0 IdPs	 High Performance Lightweight, fast and scalable
 Clustering For scalability and availability	 Themes Customize look and feel	 Extensible Customize through code	 Password Policies Customize password policies

 Sponsored by Red Hat

NonSoloSAML

- Sempre più pressante la necessità di supporto per OIDC
- Vincolo: SimpleSAMLphp
 - Provato senza successo il modulo OIDC di RedIRIS
- Ci siamo imbattuti in 



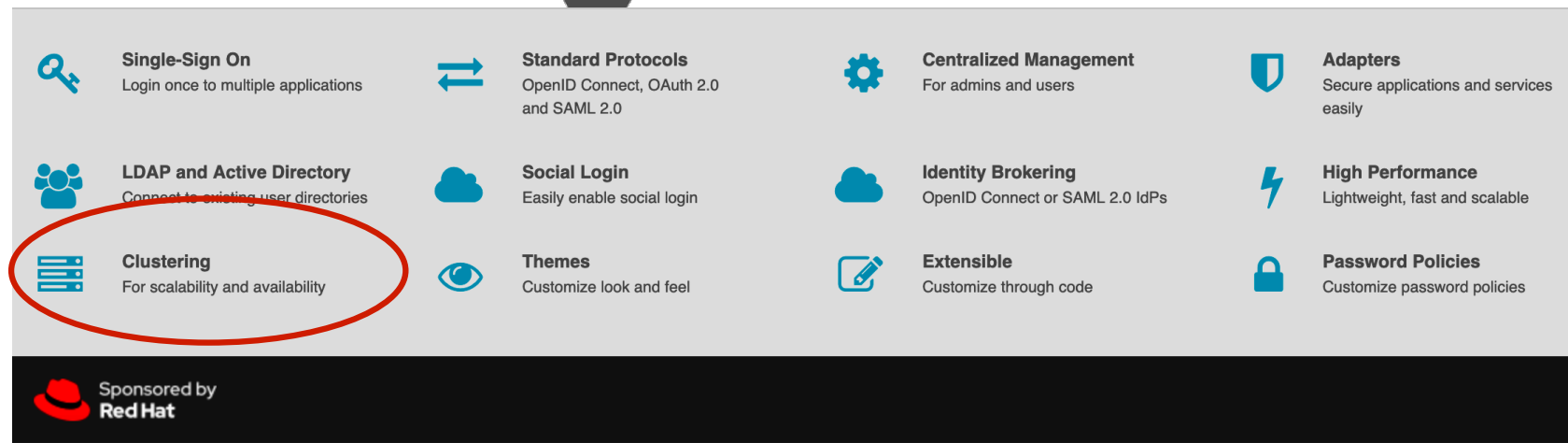
A grid of 12 Keycloak features arranged in a 3x4 layout. Each feature has an icon, a title, and a description. Two features are circled in red: 'LDAP and Active Directory' and 'Identity Brokering'.

 Single-Sign On Login once to multiple applications	 Standard Protocols OpenID Connect, OAuth 2.0 and SAML 2.0	 Centralized Management For admins and users	 Adapters Secure applications and services easily
 LDAP and Active Directory Connect to existing user directories	 Social Login Easily enable social login	 Identity Brokering OpenID Connect or SAML 2.0 IdPs	 High Performance Lightweight, fast and scalable
 Clustering For scalability and availability	 Themes Customize look and feel	 Extensible Customize through code	 Password Policies Customize password policies

 Sponsored by Red Hat

NonSoloSAML

- Sempre più pressante la necessità di supporto per OIDC
- Vincolo: SimpleSAMLphp
 - Provato senza successo il modulo OIDC di RedIRIS
- Ci siamo imbattuti in 



 Single-Sign On Login once to multiple applications	 Standard Protocols OpenID Connect, OAuth 2.0 and SAML 2.0	 Centralized Management For admins and users	 Adapters Secure applications and services easily
 LDAP and Active Directory Connect to existing user directories	 Social Login Easily enable social login	 Identity Brokering OpenID Connect or SAML 2.0 IdPs	 High Performance Lightweight, fast and scalable
 Clustering For scalability and availability	 Themes Customize look and feel	 Extensible Customize through code	 Password Policies Customize password policies

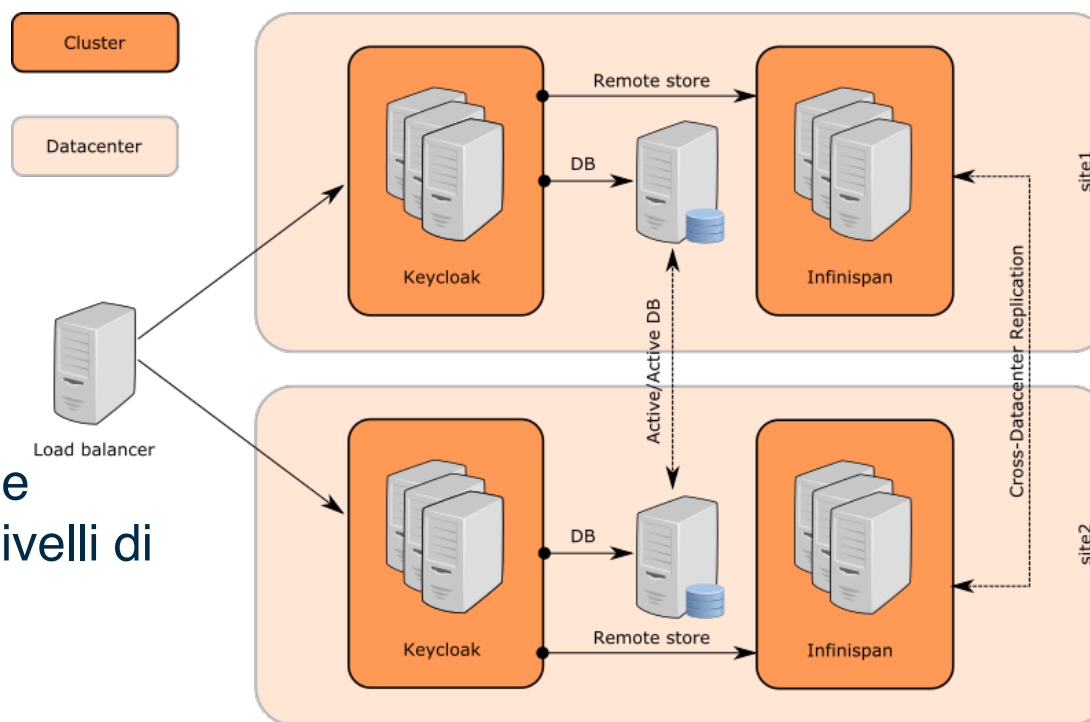
 Sponsored by Red Hat

To cluster or not to cluster...

- AuthN & AuthZ SAML
 - Distribuita
 - Scalabile
 - Fault-tolerant
- OIDC non può avere caratteristiche differenti

To cluster or not to cluster...

- AuthN & AuthZ SAML
 - Distribuita
 - Scalabile
 - Fault-tolerant
- OIDC non può avere caratteristiche differenti
- Cluster Keycloak per HA e scaling può raggiungere livelli di complessità elevati

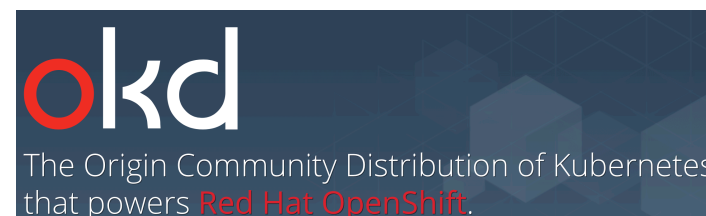


Il mio cluster è differente...



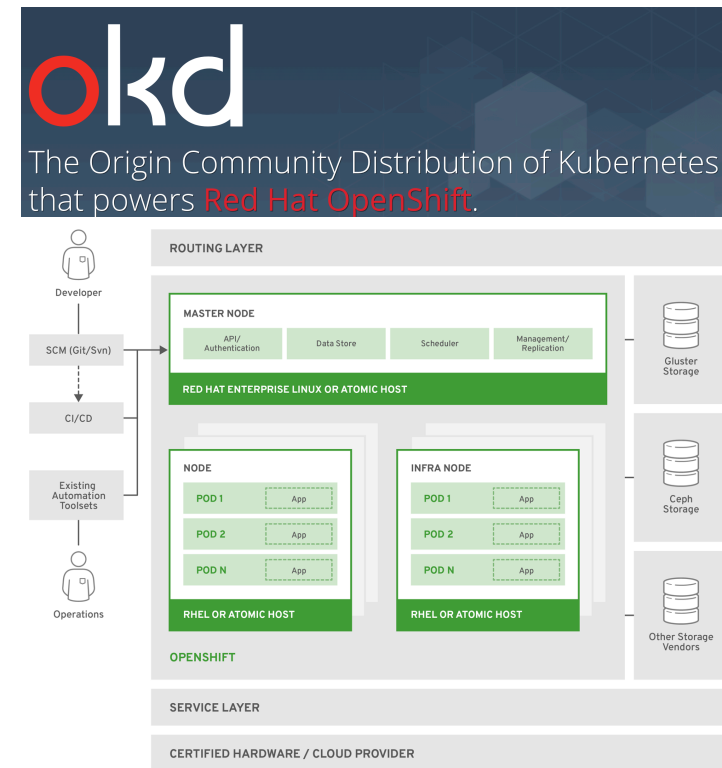
Il mio cluster è differente...

- Cluster OKD per supporto allo sviluppo ed erogazione di servizi web con architettura a microservizi.



Il mio cluster è differente...

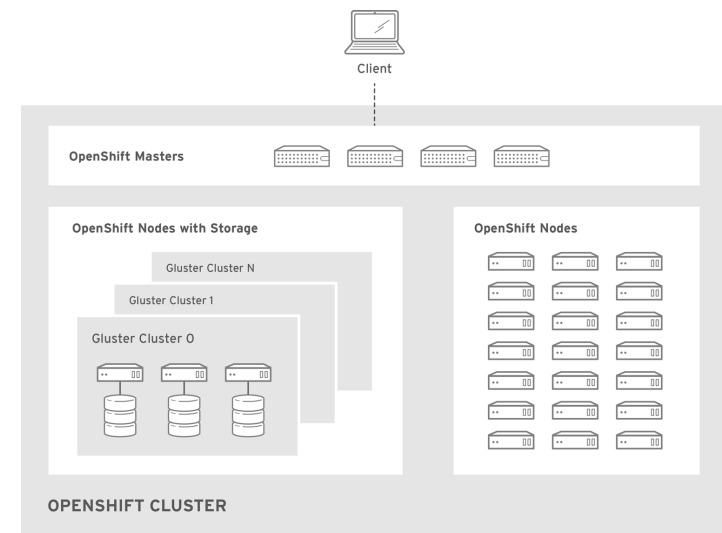
- Cluster OKD per supporto allo sviluppo ed erogazione di servizi web con architettura a microservizi.
- Architettura a layer per gestire e rendere fruibili immagini Docker



OPENSHIFT_415489_0218

Il mio cluster è differente...

- Cluster OKD per supporto allo sviluppo ed erogazione di servizi web con architettura a microservizi.
- Architettura a layer per gestire e rendere fruibili immagini Docker
- Implementabile a partire da una manciata di nodi
 - 1 master
 - 3 infrastruttura
 - GlusterFS, router, worker
- Scale-up semplice ed indolore (a caldo)



OPENSIFT_412816_0716

Keycloak Docker Image in OKD

- Disponibile immagine docker

```
docker pull jboss/keycloak
```

Keycloak Docker Image in OKD

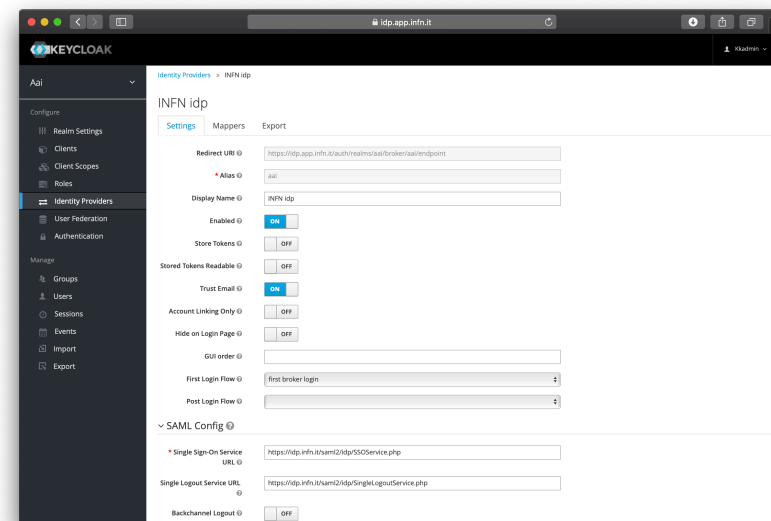
- Disponibile immagine docker
- Il servizio in OKD richiede la definizione di
 - DataBase, con relativo volume (su storage GlusterFS) e regole di accesso
 - Rotta di accesso al servizio Keycloak e regole di accesso alla console

```
docker pull jboss/keycloak
```

```
keycloak_deployment.yaml  
keycloak_route.yaml  
keycloak_secret.yaml  
keycloak_service.yaml  
postgresql_deployment.yaml  
postgresql_secret.yaml  
postgresql_services.yaml  
postgresql_volume.yaml
```

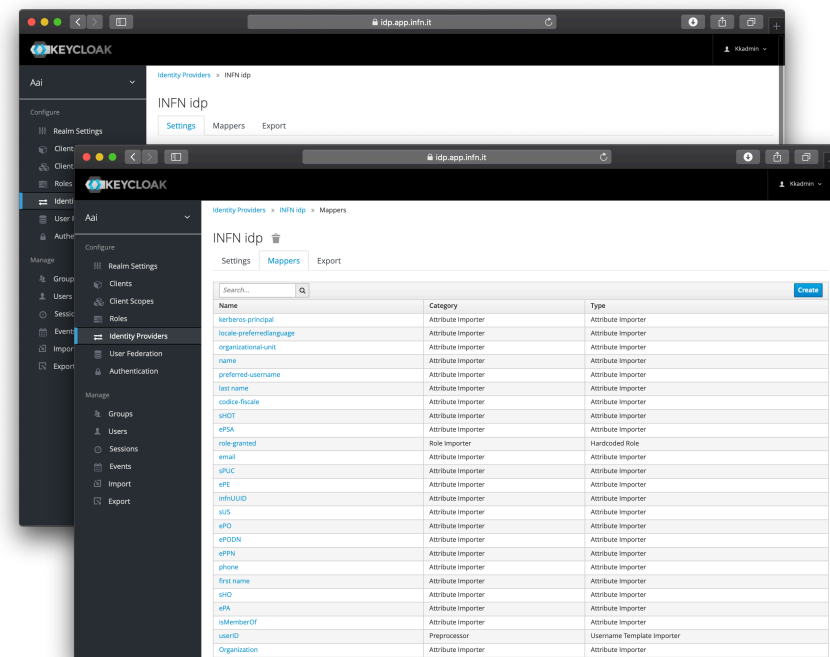
Keycloak SAML to OIDC Identity Broker

- Si configura Keycloak come SP SAML



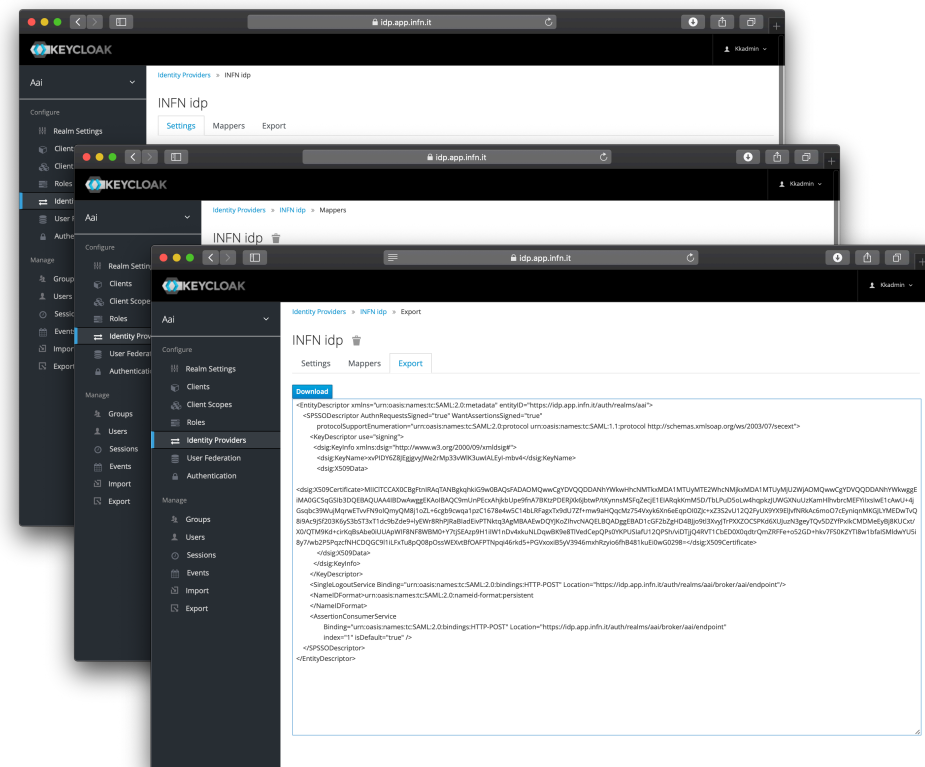
Keycloak SAML to OIDC Identity Broker

- Si configura Keycloak come SP SAML
- Si definiscono i «mapping» per gli attributi



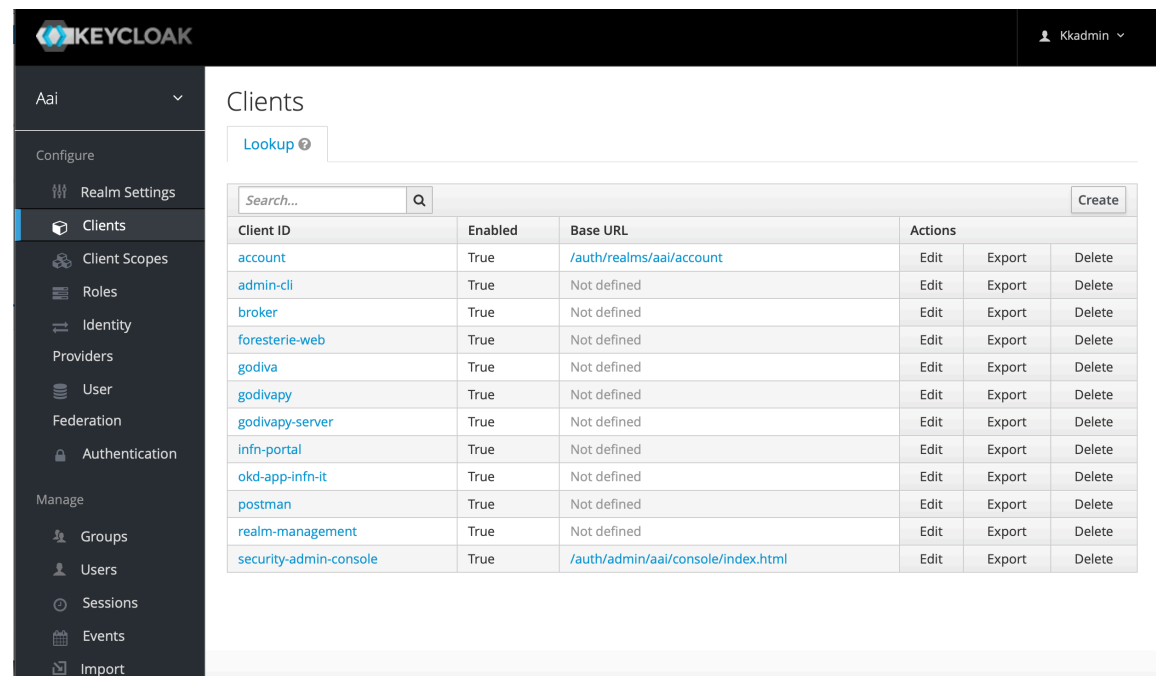
Keycloak SAML to OIDC Identity Broker

- Si configura Keycloak come SP SAML
- Si definiscono i «mapping» per gli attributi
- Si registra l'SP nell'IdP SAML



OIDC Client: browser flow

- account
 - OIDC client a corredo in Keycloak
 - /auth/realms/aai/account



KEYCLOAK Kkadmin

Aai

Configure

- Realm Settings
- Clients**
- Client Scopes
- Roles
- Identity
- Providers
- User
- Federation
- Authentication

Manage

- Groups
- Users
- Sessions
- Events
- Import

Clients

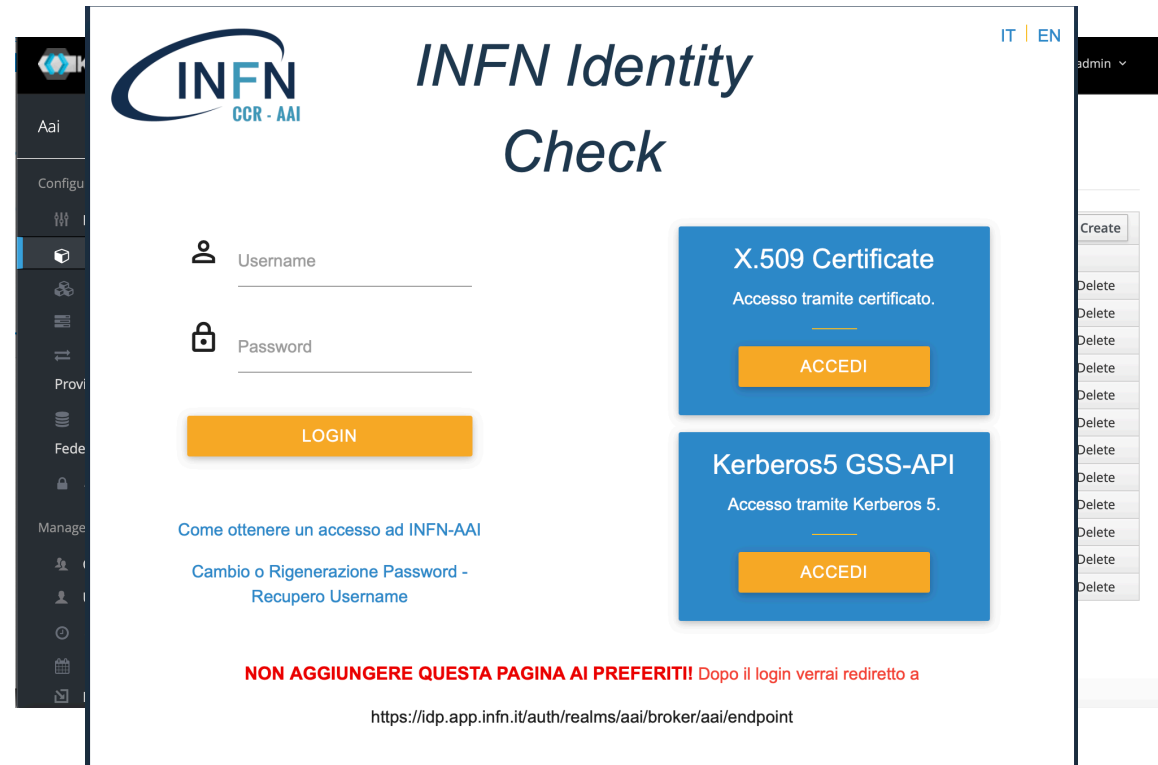
Lookup

Search...

Client ID	Enabled	Base URL	Actions		
account	True	/auth/realms/aai/account	Edit	Export	Delete
admin-cli	True	Not defined	Edit	Export	Delete
broker	True	Not defined	Edit	Export	Delete
foresterie-web	True	Not defined	Edit	Export	Delete
godiva	True	Not defined	Edit	Export	Delete
godivapy	True	Not defined	Edit	Export	Delete
godivapy-server	True	Not defined	Edit	Export	Delete
inf-n-portal	True	Not defined	Edit	Export	Delete
okd-app-inf-n-it	True	Not defined	Edit	Export	Delete
postman	True	Not defined	Edit	Export	Delete
realm-management	True	Not defined	Edit	Export	Delete
security-admin-console	True	/auth/admin/aai/console/index.html	Edit	Export	Delete

OIDC Client: browser flow

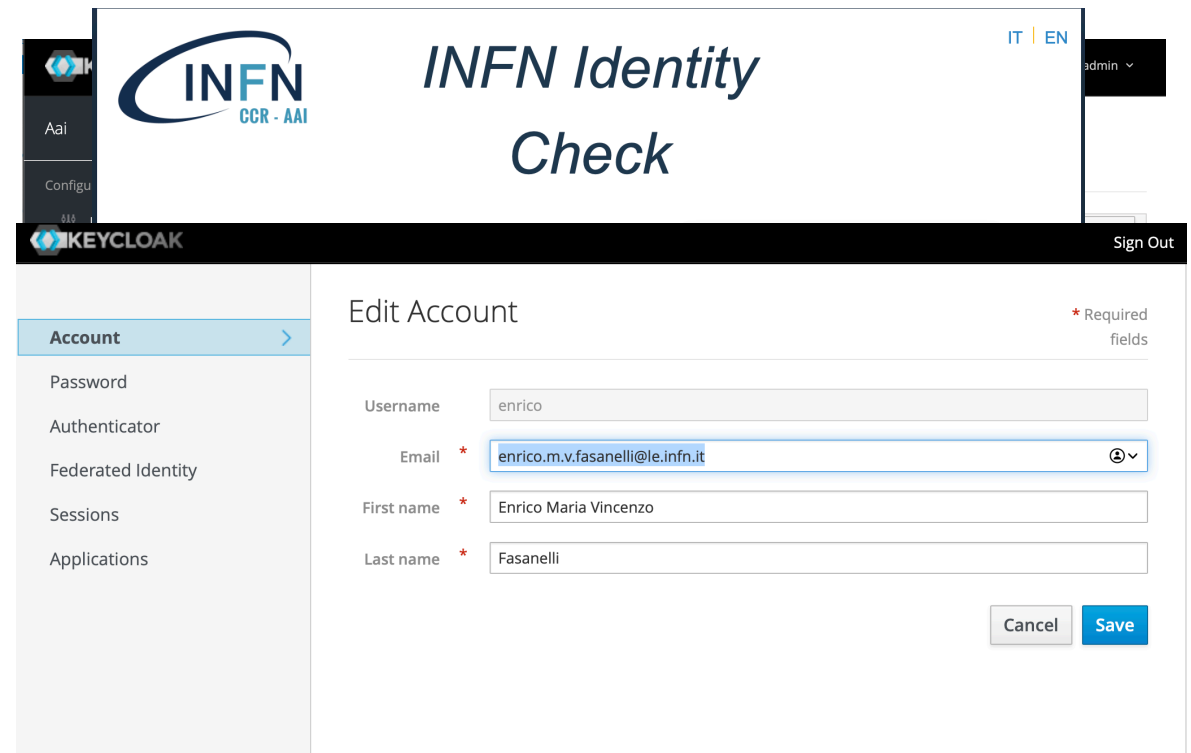
- account
 - OIDC client a corredo in Keycloak
 - /auth/realms/aai/account
- Redirect verso IdP SAML



The screenshot shows the 'INFN Identity Check' login interface. On the left is a dark sidebar with icons for Aai, Configur, and other system functions. The main content area has the INFN CCR - AAI logo at the top left. The title 'INFN Identity Check' is at the top right. Below the title are input fields for 'Username' and 'Password', each with a corresponding icon (person and lock). A large orange 'LOGIN' button is centered below these fields. To the right of the login fields are two blue boxes: 'X.509 Certificate' with the text 'Accesso tramite certificato.' and an orange 'ACCEDI' button, and 'Kerberos5 GSS-API' with the text 'Accesso tramite Kerberos 5.' and an orange 'ACCEDI' button. Below the login fields, there are links: 'Come ottenere un accesso ad INFN-AAI', 'Cambio o Rigenerazione Password -', and 'Recupero Username'. At the bottom, a red warning message states: 'NON AGGIUNGERE QUESTA PAGINA AI PREFERITI! Dopo il login verrai rediretto a' followed by the URL 'https://idp.app.infn.it/auth/realms/aai/broker/aai/endpoint'. On the far right, there is a vertical menu with 'admin' and several 'Delete' buttons.

OIDC Client: browser flow

- account
 - OIDC client a corredo in Keycloak
 - /auth/realms/aai/account
- Redirect verso IdP SAML
- First-login flow



The screenshot displays the 'INFN Identity Check' interface within a Keycloak environment. The top navigation bar includes the INFN CCR - AAI logo, language options (IT | EN), and a user profile dropdown (admin). The left sidebar shows the 'Account' menu with options: Account (selected), Password, Authenticator, Federated Identity, Sessions, and Applications. The main content area is titled 'Edit Account' and contains a form with the following fields:

- Username: enrico
- Email: * enrico.m.v.fasanelli@ie.infn.it (with a dropdown arrow)
- First name: * Enrico Maria Vincenzo
- Last name: * Fasanelli

Required fields are indicated by a red asterisk. At the bottom right of the form are 'Cancel' and 'Save' buttons. The Keycloak logo is visible in the top left of the interface.

Command Line Interface

- CLI e script sembrano essere tagliati fuori da questo ambiente, ma i system admin INFN ne hanno bisogno

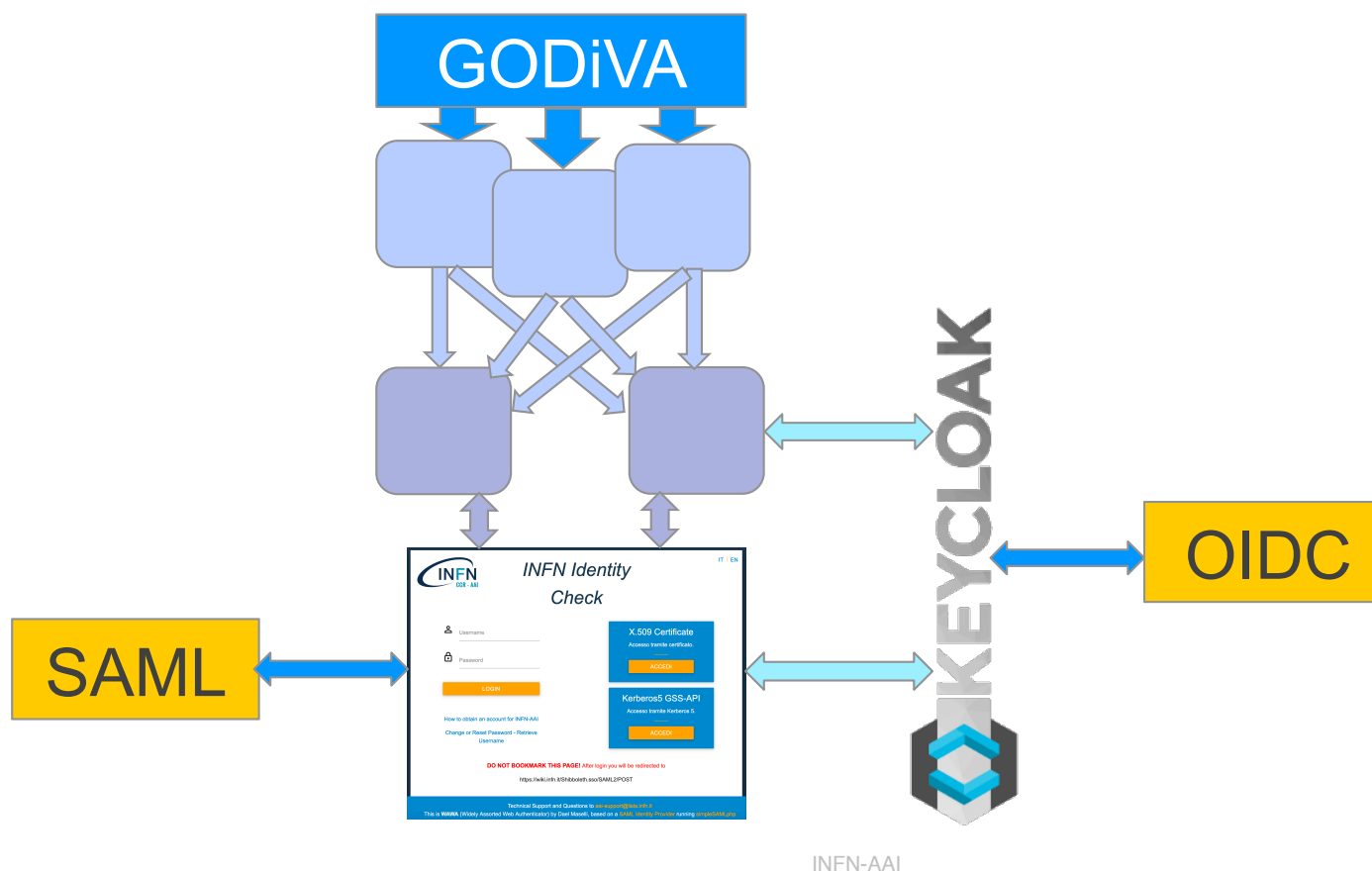


Command Line Interface

- CLI e script sembrano essere tagliati fuori da questo ambiente, ma i system admin INFN ne hanno bisogno
- OIDC Direct Grant Flow
 - LDAP back-end
- AuthZ
 - username/password
 - Kerberos



Architettura SAML + OIDC



Encoded

Decoded EDIT THE PAYLOAD AND SECRET

```

HEADER: ALGORITHM & TOKEN TYPE
{
  "alg": "RS256",
  "typ": "JWT",
  "kid":
  "SBw9c07reC7__66bjPAQoFyygBLsYgD0qKsguGaKNDc"
}

PAYLOAD: DATA
{
  "jti": "881e9ffa-1a02-4793-b889-60b93544675a",
  "exp": 1579608650,
  "nbf": 0,
  "iat": 1579608350,
  "iss":
  "https://idp.app.infn.it/auth/realms/ai-ldap",
  "sub": "5d0eb896-5203-4dca-9bbb-2ca2b561cc93:enrico",
  "typ": "Bearer",
  "azp": "godivapy-krb5",
  "auth_time": 0,
  "session_state": "035388dc-8ed0-4db6-a286-a1d16101d93a",
  "acr": "1",
  "scope": "email aai web-origins profile roles",
  "email_verified": false,
  "infnuuid": "f8d35e28-2532-43c8-989c-3fa58f85cb4",
  "name": "Enrico Maria Vincenzo Fasanelli",
  "preferred_username": "enrico",
  "given_name": "Enrico Maria Vincenzo",
  "family_name": "Fasanelli",
  "email": "enrico.m.v.fasanelli@le.infn.it",
  "client_id": "godivapy-krb5"
}

```


Grazie

- Ai colleghi INFN
 - Gruppo di Lavoro e gestione di INFN-AAI
 - Gruppo di gestione dei SSNN INFN
 - Gruppo di gestione delle reti del CNAF
 - Gruppo di Lavoro e gestione dell'infrastruttura OKD
 - Gruppo di sviluppo dei microservizi
 - Gruppo INDIGO-DataCloud per il suggerimento su Keycloak

A tutti voi per l'attenzione